NETLOGIC TRAINING CENTER

Course Training

FortiGate Basic and Advance Networking

Course Content

FortiGate Basic, will explore firewall policies, basic VPNs, antivirus, web filtering, application control, user authentication and more. These administrative fundamentals will provide you with a solid understanding of how to integrated basic network security.

FortiGate advanced networking and security is include features commonly applied in complex or larger enterprise or MSSP network, such as advance routing, transparent mode, redundant infrastructure, advanced IPSec VPN, IPS, SSO and diagnostics.

Course Objective

Upon completion of Fortigate Firewall training workshop, you'll...

- describe the capabilities of FortiGate UTM.
- Neutralize threats and misuse: viruses, torrent, and inappropriate web sites.
- Control network access based on device type.
- Authenticated user through firewall policies.
- Apply port forwarding, source NAT and destination NAT.
- Offer and SSL VPN for secure access to your private network.
- Establish and IPSec VPN Tunnel between two FortiGate appliance.
- Compare policy-base to tunnel-base IPSec VPN.
- Interpret log entries.
- Generate Reports.
- Use the GUI and CLI for administration.
- Deploy the right operation mode.
- Deploy an explicited proxy with firewall policies, authentication and caching.
- Evolve beyond port numbers with application control.
- Deploy FortiGate devices as an HA cluster for fault-tolerance and high performance.
- Inspect traffic transparently, forwarding as a Layer 2 device.
- Analyze a FortiGate 's route table.
- Connect virtual domain (VDOMs) without packet leaving the FortiGate.
- Offer Fortinet Single Sign ON (SSO) access to network services, integrated with Microsoft Active Directory.
- Inspect SSL/TLS-secured traffic to prevent encryption use to bypass security policies
- Fortinet DMZ deployment and configuration

Course Prerequisite

- Knowledge of OSI Layer
- Knowledge of firewalling concept in an IPv4 Network concepts

Course Pre-Test

Not Required

Course Details

Day 1

Item	Subject	Details	Personal Lab and devices	Workgroup Lab and devices
1	Fortigate Overview	- Overview and Design - initial Access to Fortigate Firewall - Overview of interface and features	Theory & Lecture	
2		- Internal (LAN) interface - External (WAN) interface - DMZ zone Interface - General Setting	Theory & Lecture	
		Break		
3	Routing and Upgrade	- OSPF Routing - Confirm Basic Internet Access - Upgrade Firmware	Theory & Lecture	
4	Filtering and SSL Decryption operation	- Filtering based on Network and Services - Filtering Base on URL - SSL Decryption	Theory & Lecture	
	Summary challenge advance lab for factory default and Basic Firewall configuration, Routing , Upgrade and Filtering	Lab 1 - Factory default Fortigate firewall - Password Recovery and Initial Configuration - Removing the Existing Configuration Lab 2 - Analyzing the Base Configuration and Saving It - Basic configure Fortigate Firewall - Configure DMZ Zone and apply policy DMZ - General Setting and investigate operation Lab 3 - Configure Routing protocol on Fortigate Firewall - Monitoring Firewall Operation Lab 4 - Configure Filtering base on network service and URL - Configure SSL Decryption and Monitoring Firewall Operation	(Lab 1 and Lab 2) **Real Device** ISR router 4321 1 Unit Catalyst 3560-CX 1 Unit Firewall Fortigate 60D 1 unit	

Day 2

Item	Subject	Details	Personal Lab and devices	Workgroup Lab and devices
5	Filtering and QoS	- Anti-Virus Blocking - Traffic Shaping (per-IP) - Filtering based on Applications	Theory & Lecture	
6	Synchronization with AD and Filtering base AD information	- LDAP using Active Directory - Filtering based on User Identify (Active) - Filtering based on User Identify (Passvie) using FSSO	Theory & Lecture	
		Break		
7	NAT and Remote Access SSL VPN	- Static NAT (New IP) and Policy - Static NAT Port forwarding (WAN IP) and Policy - Remote Access using SSL VPN	Theory & Lecture	
8	Site to Site VPN with Cisco and IPsec VPN	- Site VPN Tunnel to Cisco IOS Router - Remote Accsss using IPSec - VLAN tagging and Zones	Theory & Lecture	
	Summary challenge advance lab for Qos and AD Synchronization, Remote and Site to Site VPN	Lab 1 - Configure QoS (Traffic Shaping(with Application - Filtering configure base on Critical Applications Lab 2 - Configure LDAP on Windows AD and Synchronization with Fortigate Firewall - Filtering configure base on AD information Lab 3 - Remote Access VPNs - Configure a Web-Based SSL VPN - Configure static nat and monitoring Lab 4 - Configure Site-to-Site VPNs to router Cisco - Configure Remote Access with IPSec to router Cisco	(Lab 1 and Lab 2) **Real Device** router 4321 1 Unit Catalyst 3560-CX 1 Unit Firewall Fortigate 60D 1 unit Windows AD 1 Unit	

Day 3

Item	Subject	Details	Personal Lab and devices	Workgroup Lab and devices
9	Fortigate High Availability with Gateway Redundancy	- High Availability (HA) concept - Standard Protocol for HA - Fortigate HA mechanism	Theory & Lecture	
10	Fortigate Network Load Balancing	- Load Balance feature explain - Fortigate Load Balancing - Operation Load Balancing and fine tune	Theory & Lecture	
		Break		
11	DHCP and Guest Services	- DHCP Service - Guest service using Captive Portal - Guest Network - Policies to Internet	Theory & Lecture	
12	IPS , VDOM operations	- Intrusion Prevention (IPS) - Virtual Domain (VDOM) - Forticloud	Theory & Lecture	
	Summary challenge advance lab for Network Service and IPS	Lab1 - Configure network service DHCP and monitoring - Configure Guest Service by Captive Portal and Policies Lab 2 - Configure HA and Network Load Balance - Tuning Load Balancing Lab 3 - Enabling IPS on Fortigate Firewall - Enabling VDOM and monitoring operation	(Lab 1 – Lab 3) **Real Device** router 4321 1 Unit Catalyst 3560-CX 1 Unit Firewall Fortigate 60D 1 unit Windows AD 1 Unit	

Course Post-Test

Not Required

Course Materials

Not include in this class training (but you can requested from sale team)

Course Devices Training (Per 1 Person)

Cisco Catalyst 3560-CX

Cisco Router ISR 4321

Fortigate firewall 60E

Windows Server
Active Directory